

Rochester Institute of Technology

RIT Scholar Works

Theses

5-2017

Algorithmic Framework and Implementation of Spectrum Holes Detection for Cognitive Radios

Ian J. Frasch
ijf1860@rit.edu

Follow this and additional works at: <https://scholarworks.rit.edu/theses>

Recommended Citation

Frasch, Ian J., "Algorithmic Framework and Implementation of Spectrum Holes Detection for Cognitive Radios" (2017). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.

Algorithmic Framework and Implementation of Spectrum Holes Detection for Cognitive Radios

by

Ian J. Frasch

A Thesis Submitted in Partial Fulfillment of the Requirements for the
Degree of Master of Science
in Computer Engineering

Supervised by

Dr. Andres Kwasinski
Department of Computer Engineering
Kate Gleason College of Engineering
Rochester Institute of Technology
Rochester, New York
May 2017

Approved by:

Dr. Andres Kwasinski
Thesis Advisor, Department of Computer Engineering

Dr. Panos Markopoulos
Committee Member, Department of Electrical Engineering

Dr. Marcin Lukowiak
Committee Member, Department of Computer Engineering

Abstract

Algorithmic Framework and Implementation of Spectrum Holes Detection for Cognitive Radios

Ian J. Frasch

The ability to dynamically discover portions of unused radio spectrum (spectrum holes) is an important ability of cognitive radio systems. Spectrum holes present a potential opportunity for wireless communication. Detection of holes and signals allows cognitive radios to dynamically access and share the spectrum with minimal interference. This work steps through the design, implementation, and analysis of a spectrum holes detector for cognitive radios. Energy detection and cyclostationary detection algorithms for detecting spectrum holes are compared through computer simulations. Ultimately an energy detection algorithm is proposed which performs better than the cyclostationary detection algorithm and requires no a-priori knowledge of noise power. The energy detection algorithm is implemented on the bladeRF x115 software-defined radio for wideband detection, leveraging on-board FPGA hardware and field-programmable analog hardware to scan a gigahertz-order range of frequencies and discover spectrum holes in real time. Resource utilization and requirements of the implementation are analyzed, and a utilization of 8.8% of the FPGA's logic resources is reported. Experiments are performed on the implementation to measure its detection performance and demonstrate its ability to detect holes over a wide bandwidth with reasonable latency.

Contents

Abstract	ii
Acronyms	ix
1 Introduction	1
1.1 Cognitive Radio	2
1.1.1 Regulatory Compliance	3
1.1.2 Potential Applications	3
1.1.3 Current State	4
1.2 Contribution of Thesis	4
2 Background	6
2.1 Energy Detection	6
2.1.1 Advantages	7
2.1.2 Drawbacks	8
2.2 Cyclostationary Detection	8
2.2.1 Spectral Correlation Density (SCD)	8
2.2.2 Spectral Coherence	9
2.2.3 Gallery of Spectral Coherence	10
2.2.4 Existing Work	11
2.2.5 Advantages	12
2.2.6 Drawbacks	13
2.3 Detector Performance Metrics	13
3 Detection Algorithm	15
3.1 Single-Band Energy Detection Algorithm	15

3.2	Single-Band Cyclostationary Detection Algorithm	16
3.3	Simulation of Single-Band Algorithms	18
3.3.1	Setup	18
3.3.2	Results	20
3.3.3	Conclusion	21
3.4	Multiband Detection Algorithm	22
3.5	Simulation of Multiband Algorithm	24
3.5.1	Results	24
3.5.2	Remarks for Implementation	25
4	Implementation	27
4.1	SDR Platform	27
4.2	Implementation Overview	28
4.3	Implementation Architecture	30
4.3.1	Hardware datapath	31
4.3.2	Nios software	31
4.3.3	PC interface	31
4.4	Details	32
4.4.1	Design	32
4.4.2	DC Offset Handling	32
4.4.3	Fixed-point Bit Growth	33
4.4.4	Antenna and Frequency Considerations	33
4.5	Resource Utilization	34
4.6	Requirements for Implementation	34
4.7	Source Code	35
5	Experiments and Results	36
5.1	Implementation Issues	36
5.1.1	Spurious Tones in Noise Spectrum	36

5.1.2	Analog Filter Frequency Response	37
5.2	Side Experiment: Noise Characterization	37
5.2.1	Noise Floor Variation	37
5.2.2	PSD and Spectral Coherence of Noise	38
5.3	Setup of Performance Experiments	39
5.3.1	Detector Parameters and Characteristics	40
5.4	Results	41
5.4.1	Single Transmission	41
5.4.2	Multiple Transmissions	43
5.4.3	Example Detector Output	43
6	Conclusion	45
	Bibliography	46

List of Tables

3.1	Setup of QPSK and OFDM Test Signals	18
4.1	Implementation Specifications and Settings	30
4.2	FPGA Resource Utilization of Hole Detector	34
5.1	Detector Parameters and Characteristics	40

List of Figures

1.1	Dynamic discovery of spectrum holes [1]	1
1.2	IEEE 802.22 Wireless Regional Area Network (WRAN) cell with base station and user terminals [2].	3
2.1	PSD and spectral coherence estimates of 4-FSK signal at SNR = 5 dB.	10
2.2	PSD and spectral coherence estimates of 16-QAM signal at SNR = 15 dB.	11
2.3	PSD and spectral coherence estimates of 16-QAM signal at SNR = -5 dB.	11
2.4	PSD and spectral coherence estimates of white Gaussian noise.	11
3.1	PSD and spectral coherence of 9216-sample QPSK test sig- nal at SNR = 15dB (F_s is the sampling frequency).	19
3.2	PSD and spectral coherence of 9216-sample OFDM test sig- nal at SNR = 15dB (F_s is the sampling frequency).	19
3.3	PSD and spectral coherence of 9216-sample QPSK test sig- nal at SNR = -5dB (F_s is the sampling frequency).	20
3.4	Probability of Detection vs SNR with fixed $P_{FA}=0.1$ for (a) QPSK test signal and (b) OFDM test signal.	20
3.5	Detector ROC curves with fixed SNR for (a) QPSK test sig- nal with SNR = -10 dB and (b) OFDM test signal with SNR = 5 dB.	21

3.6	Performance of multiband energy detection algorithm. (a) Average percentage of signal power detected in signal's bandwidth vs in-band SNR (b) Probability of detecting at least 90% of the power in signal's bandwidth vs in-band SNR . . .	25
3.7	Effects on detection performance (a) increased sensing time (and therefore number of FFT averages) and (b) decreased FFT size.	25
4.1	Block diagram of receive chain in the bladeRF implementation platform	27
4.2	Image of bladeRF device	28
4.3	Method of operation for scanning wide bandwidth: example with 3 frequencies. Illustrates the sensing time (per band), retune time, and instantaneous bandwidth of the receiver BW_I	29
4.4	Implementation Architecture	30
5.1	PSD and spectral coherence estimates of real noise received with the bladeRF	38
5.2	Experimental Setup	39
5.3	Detector performance for a single continuous transmission and fixed $P_{FA} = 0.09$	42
5.4	Detector ROC curve for a single continuous transmission and fixed in-band SNR = -6 dB	42
5.5	Detector performance for three continuous transmissions . .	43
5.6	Real-time output from the detector with three wired QPSK transmissions with bandwidths of 5 MHz. (a) Scaled power spectral density; (b) Detected holes; (c) Rankings of detected holes.	44

Acronyms

ADC Analog to Digital Converter

AWGN Additive White Gaussian Noise

CD Cyclostationary Detection

DAC Digital to Analog Converter

DC Direct Current

ED Energy Detection

FFT Fast Fourier Transform

FPGA Field Programmable Gate Array

GPIO General Programmable Interface

IQ In-phase/Quadrature

OFDM Orthogonal Frequency Division Multiplexing

PD Probability of Detection

PFA Probability of False Alarm

PSD Power Spectral Density

PSK Phase Shift Keying

QAM Quadrature Amplitude Modulation

RF Radio Frequency

ROC Receiver Operating Characteristic

SC Spectral Coherence

SCD Spectral Correlation Density

SDR Software-Defined Radio

SMA SubMiniature version A

SNR Signal to Noise Ratio

SPI Serial Peripheral Interface

UART Universal Asynchronous Receiver/Transmitter

VHDL Very High Speed Integrated Circuit Hardware Description Language

Chapter 1

Introduction

The ability to dynamically discover portions of unused radio spectrum (holes) and utilize those holes leads to wireless communication which is faster, more reliable, and more efficiently uses the spectrum. Dynamic sensing of the spectrum can reduce interference, which is especially important in the present day world which is filled with wireless communication systems constantly transmitting. Dynamic spectrum access (DSA) refers to dynamically switching operating frequency and/or bandwidth to use available spectrum holes. The concept of dynamic spectrum access is illustrated in Figure 1.1. Regulation of the radio spectrum has caused an apparent spectrum scarcity, which is challenging for the launch of new wireless services such as 5G cellular networks. However, this scarcity is an artificial limitation since significant portions of licensed spectrum are unoccupied most of the time. Systems are needed which can employ dynamic spectrum access to utilize spectrum holes, overcoming the problem of spectrum scarcity.

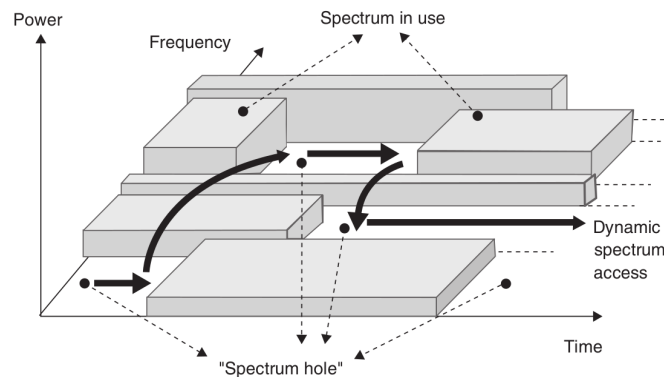


Figure 1.1: Dynamic discovery of spectrum holes [1]

1.1 Cognitive Radio

Cognitive radio refers to an emerging field of intelligent wireless communication systems which adapt their transmission/reception parameters based on the environment. A cognitive radio is meant to be aware of its environment, producing reliable communication whenever and wherever needed and efficiently use the radio spectrum. In addition to spectrum sensing for dynamic spectrum access, cognitive radios employ channel estimation and transmit power control to reduce interference with other radios. Based on changes in input stimuli, cognitive radios adapt communication parameters such as carrier frequency, bandwidth, modulation scheme or strategy, and transmit power. Decisions are made using learning and reasoning. The primary goal of cognitive radio is to dynamically share the spectrum for efficient spectrum use, eliminating spectrum scarcity. Cognitive radio is built on software-defined radio (SDR), a flexible and reconfigurable radio platform which is commercially available today. The detection of spectrum holes is a defining ability of a cognitive radio system, allowing it to find vacant frequency bands and avoid interfering with other users [3].

A cognitive radio contrasts with traditional radios which use a fixed portion of allocated spectrum and contain fixed functionality hardware. When a traditional radio is not transmitting, the spectrum it has been licensed to use is wasted since it cannot be used by anyone else. Cognitive radios are meant to reduce this wasted spectrum by dynamically sharing the spectrum; leading to more efficient overall spectrum use. The spectrum can be shared both with licensed transmitters (primary users) and with other cognitive radios (secondary users) .

Although spectrum allocation from government regulatory agencies has caused the spectrum to appear scarce, large portions of the spectrum may be unused at any given time or location. Cognitive radio hopes to take advantage of this unused spectrum to increase the opportunity for wireless communications, increase data rates because of larger available bandwidth, and reduce interference between neighboring transmitters.

1.1.1 Regulatory Compliance

In the United States, large portions of spectrum inside the 54 MHz - 862 MHz region were made available when the Federal Communications Commission (FCC) ordered the termination of analog television transmission in the 2009 digital switchover mandate. The FCC has authorized unlicensed transmitters to use these frequencies, also known as white spaces, provided they do not interfere with a licensed service [4]. This provides legal opportunity for cognitive radios to thrive. In the future more areas of the spectrum may be opened up to unlicensed cognitive transmitters, allowing more opportunity for communication.

1.1.2 Potential Applications

Cognitive radio networks have been standardized in IEEE 802.22: Wireless Regional Area Networks (2011). This standard outlines specifications for cognitive radio networks which operate in TV bands between 54 MHz and 862 MHz, sharing spectrum with licensed TV broadcasters [2]. The standard envisions a wireless network employed in rural locations to provide broadband internet access, illustrated in Figure 1.2.

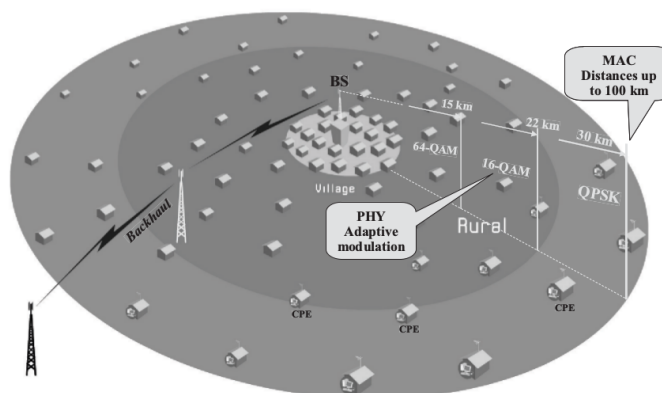


Figure 1.2: IEEE 802.22 Wireless Regional Area Network (WRAN) cell with base station and user terminals [2].

1.1.3 Current State

Theoretical research on cognitive radio is abundant, software-defined radios are commercially available, white space frequencies are legally available, and there is even an IEEE standard, but cognitive radios are still not yet out of the laboratory for everyday commercial use. It seems that the missing piece of the puzzle is implementation. Implementation-focused research can help make the vision of cognitive radios a reality.

1.2 Contribution of Thesis

This thesis is focused on implementation of the spectrum hole detection ability of cognitive radios. Existing research covers theoretical methods of sensing the radio spectrum and detecting holes/signals, but lacks content on implementations (especially wideband implementations) and implementation issues. Existing research also tends to lack algorithms that could realistically be implemented to scan a gigahertz-order range of frequencies to blindly detect signals. Implementation feasibility of algorithms is typically not discussed.

There is a need for research which focuses on implementation of spectrum hole detection and its related issues, including hardware requirements. Software-defined radios with reconfigurable digital and analog hardware have the ability to operate over an extremely wide range of frequencies, making them ideal for sensing a large bandwidth of radio spectrum for cognitive purposes. The purpose of this research is to design, document, and implement a wideband spectrum holes detector on software-defined radio. This research will focus on developing and demonstrating a working implementation suitable for cognitive radios. We will describe in detail its design as well as its requirements in terms of hardware/software resources. This research hopes to advance the developmental state of cognitive radios and bring them closer to everyday use.

This thesis is organized as follows: Chapter 2 provides the theoretical and mathematical background of existing spectrum hole detection techniques. Chapter 3 describes the design of a spectrum hole detection algorithm using MATLAB simulation studies to assess performance. Chapter 4 details real-time implementation of the algorithm on the bladeRF x115 software-defined radio, utilizing on-board FPGA hardware for processing. Chapter 5 describes experiments performed on the implementation to assess its performance and uncover implementation issues, as well as experimental outcomes.

Chapter 2

Background

Spectrum hole detectors for cognitive radios detect the presence of transmission signals across a wide range of frequencies and assert that holes exist in frequencies where signals are absent. Typically detection must be performed without any a-priori knowledge of the signals to be detected. This type of detection is referred to as blind detection. Matched filter detection is considered the optimum technique for signal detection [5], but is not discussed in this thesis because it is a non-blind technique which requires complete knowledge of the signals to be detected. The two primary techniques for blind spectrum hole detection are energy detection and cyclostationary feature detection [6]. Energy detection is the most common and straightforward approach; it refers to observing the spectral energy (or power) at different frequencies and using a threshold to decide if a signal is present at each frequency. The potential problem with energy detection is that it requires accurate estimation of the spectral noise floor in order to choose the detection threshold. Cyclostationary feature detection refers to taking advantage of the innate spectral correlation that exists in transmission signals and not in noise. Cyclostationary feature detection typically involves extraction of peaks or features in the computed spectral correlation density.

2.1 Energy Detection

Energy detection involves observing the spectral energy across the visible spectrum and using a threshold to decide if a signal is present at each frequency. Energy detection typically involves the use of the power spectral density (PSD) of the input signal as a detection statistic. The PSD, denoted by $S_{xx}(f)$, can be estimated using the average squared magnitude of the

truncated Fourier transform, as shown in equation 2.1.

$$S_{xx}(f) = \lim_{T \rightarrow \infty} \frac{E[|X_T(f)|^2]}{T} \quad (2.1)$$

where $E[\cdot]$ is the expectation operator and $X_T(f)$ is the truncated Fourier transform of the input time-domain signal $x(t)$:

$$X_T(f) = \int_{-T/2}^{T/2} x(t)e^{-j2\pi ft} dt \quad (2.2)$$

To determine if a signal is present, the PSD values are compared to the detection threshold which is set based on the noise power. In frequencies where the PSD value exceeds the threshold, the energy detector asserts that a signal is present:

$$S_{xx}(f) \geq Threshold : \text{signal present} \quad (2.3)$$

Energy detection algorithms for cognitive radios are proposed in [7] and [8]. For best performance in practice, energy detectors should use the highest number of Fourier transform averages possible. Increasing the number of averages will produce a more accurate PSD estimate at the cost of a longer sensing time (meaning longer signal length). As the number of averages is increased, the PSD estimate of white Gaussian noise approaches a flat horizontal line.

2.1.1 Advantages

Energy detection has the advantage of being low in complexity, and efficient for implementation using the fast Fourier transform algorithm. Energy detection algorithms also never require a-priori information about the signals to be detected, and therefore can always be applied for blind detection.

2.1.2 Drawbacks

An inaccurate estimate of in-band noise power can reduce performance from the energy detector. For example, if the noise power estimate is too high, the chosen detection threshold will be higher, causing a decreased probability of signal detection. The work in [9] and [10] quantifies the effect of uncertain noise power estimates on performance of energy detectors. Noise power estimation can be difficult in practice, especially since (1) the power of noise generated by RF front ends can vary over frequency, (2) the noise floor can also consist of external (background) noise in addition to thermal noise, and (3) thermal noise power varies over temperature.

2.2 Cyclostationary Detection

A cyclostationary signal is defined as a random process with periodic mean and autocorrelation. Cyclostationarity causes spectral correlation: meaning the magnitude and phase of different frequency components of the signal are correlated over time. The spectral correlation between different frequencies is given by the spectral correlation density (SCD). Cyclostationary detection identifies signals by looking for peaks or shapes in the computed SCD or spectral coherence (a normalized version of the SCD). Stationary noise does not exhibit spectral correlation, and therefore its theoretical SCD would be zero.

2.2.1 Spectral Correlation Density (SCD)

The spectral correlation density (also referred to as the cyclic spectrum or spectral correlation function) is a two-dimensional function representing the correlation between different frequency components as they change over time. The SCD is a function of frequency f and cyclic frequency α . The SCD output is the correlation (inner product) between frequency components located at $(f + \alpha/2)$ and $(f - \alpha/2)$. When $\alpha = 0$ the SCD reduces to

the power spectral density. Formally, the SCD is given by

$$S_x^\alpha(f) = \lim_{T \rightarrow \infty} \lim_{\Delta t \rightarrow \infty} \frac{1}{\Delta t} \int_{-\Delta t/2}^{\Delta t/2} \frac{1}{T} X_T(t, f + \alpha/2) X_T^*(t, f - \alpha/2) dt \quad (2.4)$$

where X_T is the finite-time Fourier transform of the the input time-domain signal $x(u)$; representing the Fourier transform over time:

$$X_T(t, f) = \int_{t-T/2}^{t+T/2} x(u) e^{-j2\pi f u} du \quad (2.5)$$

2.2.2 Spectral Coherence

Spectral coherence is a useful detection statistic derived from the SCD. Spectral coherence is a normalized version of the SCD which ranges between 0 and 1 in magnitude. It is essentially the correlation coefficient for the SCD. Spectral coherence is given by

$$C_x^\alpha(f) = \frac{S_x^\alpha(f)}{\sqrt{S_x^0(f + \alpha/2) S_x^0(f - \alpha/2)}} \quad (2.6)$$

where $S_x^\alpha(f)$ is the spectral correlation density, with parameter α .

Conceptually, the spectral coherence represents the correlation between two frequency components located at $(f + \alpha/2)$ and $(f - \alpha/2)$ normalized by the PSD at each frequency.

Spectral coherence is useful because it essentially removes the PSD from the picture, leaving only spectral correlation. If the gain of the entire received signal (including noise) is increased, the magnitude of the Fourier transform will be scaled up, causing SCD values to be scaled up as well. However, the spectral coherence would not change. Additionally, the mean magnitude of the SCD estimate of a snapshot of raw noise will change based on the noise power; meaning the use of the SCD magnitude as a detection statistic would require a noise power estimate. The spectral coherence of a snapshot of raw noise (of fixed signal length) always contains the same

mean magnitude regardless of the noise power. This means that no noise power estimate is needed. The spectral coherence magnitude of a signal only depends on its SNR. This lends the ability to set a fixed detection threshold without having to worry about changing noise levels or changing gain.

2.2.3 Gallery of Spectral Coherence

Figures 2.1, 2.2, 2.3, and 2.4 show examples of spectral coherence estimates computed in MATLAB, along with corresponding PSD estimates. The spectral coherence corresponding to $\alpha = 0$ has been omitted since it is always equal to 1. Each input signal had a length of 9216 samples. Root-raised cosine pulse shaping was applied to the 16-QAM signal. The 16-QAM signal was modulated at 4 samples per symbol, and the 4-FSK signal was modulated at 16 samples per symbol. Distinct features are clearly visible in the spectral coherence of the signals at high SNR, shown in Figures 2.1 and 2.2. Observe in Figure 2.3 that the features in the spectral coherence of the 16-QAM signal are diminished in low SNR. Observe that in Figure 2.4 the the magnitude of the spectral coherence estimate of white Gaussian noise is slightly above zero. This is due to the finite signal length of 9216 samples. A longer signal length would produce more accurate spectral coherence estimate at the cost of a longer sensing time in practice. As the signal length is increased, the spectral coherence estimate of noise approaches zero, and the PSD estimate of noise approaches a flat horizontal line.

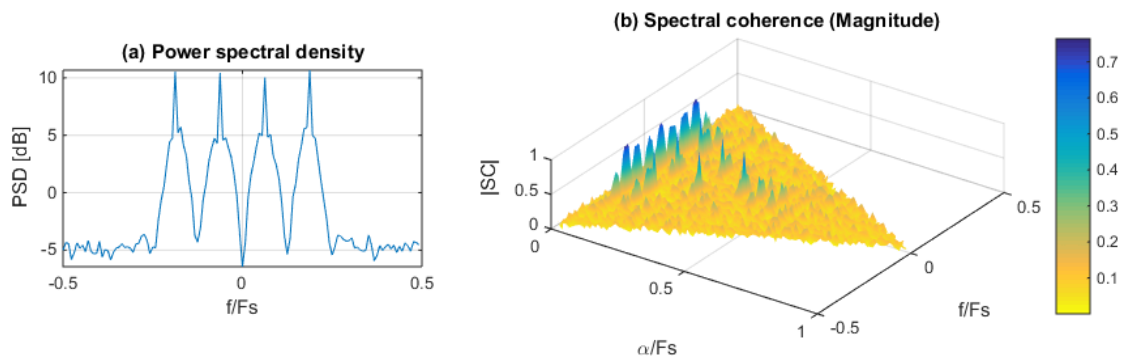


Figure 2.1: PSD and spectral coherence estimates of 4-FSK signal at SNR = 5 dB.

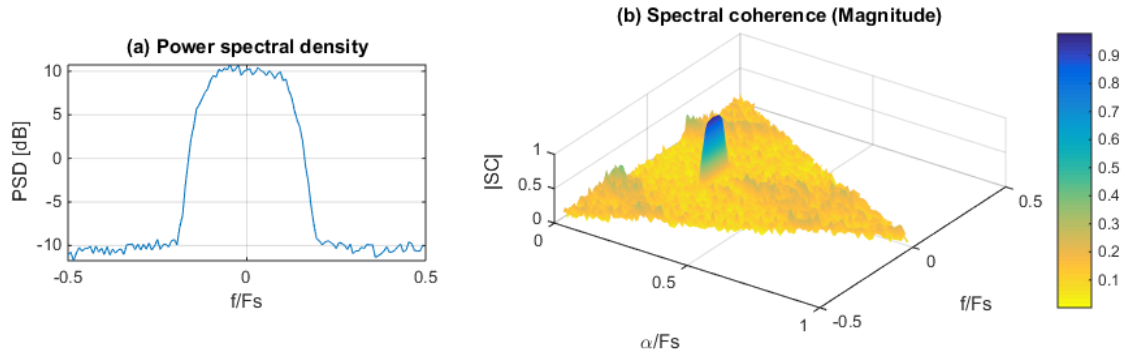


Figure 2.2: PSD and spectral coherence estimates of 16-QAM signal at SNR = 15 dB.

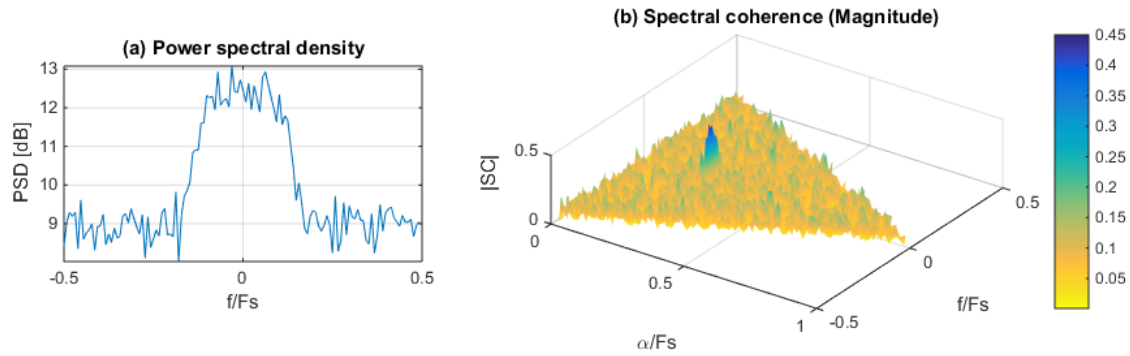


Figure 2.3: PSD and spectral coherence estimates of 16-QAM signal at SNR = -5 dB.

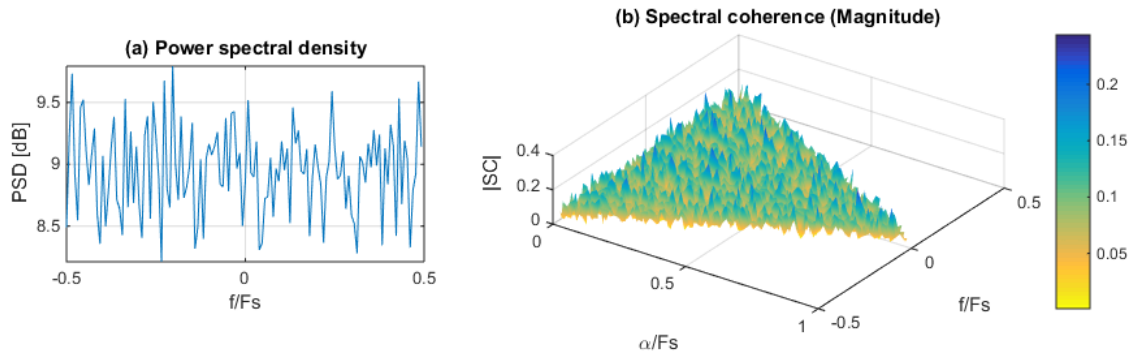


Figure 2.4: PSD and spectral coherence estimates of white Gaussian noise.

2.2.4 Existing Work

Cyclostationary detection algorithms include blind detection algorithms and non-blind detection algorithms. In blind detection algorithms, no a-priori information such as carrier frequency, modulation, and bandwidth is required

about the signals to be detected. Non-blind techniques are not useful for the general purpose spectrum sensing needed by cognitive radios. Existing work in blind detection algorithms includes the work in [11], which uses the squared magnitude of the spectral coherence as a detection statistic, then uses a threshold test to determine if a signal is present:

$$|C_x^\alpha(f)|^2 \geq Threshold : \text{signal present} \quad (2.7)$$

For blind detection, the work in [12] suggests using the crest factor of the α -domain profile as a detection statistic, where the α -domain profile $I(\alpha)$ is defined as the maximum observed $C_x^\alpha(f)$ magnitude for each α . The crest factor (CF) is defined as the ratio of peak amplitude to root-mean-square amplitude:

$$I(\alpha) \triangleq \max_f |C_x^\alpha(f)| \quad (2.8)$$

$$CF(I(\alpha)) \geq Threshold : \text{signal present} \quad (2.9)$$

For non-blind detection, the work in [13] suggests integrating the SCD over a "feature mask" to detect signals, where the feature mask restricts the integration to the range of values for (α, f) values where peaks/features are expected. This requires the receiver to know a-priori the frequency and theoretical SCD of the input signal, and therefore cannot be used for blind detection.

Research in [14] and [15] suggests using cyclostationary detection for fine sensing (with a long sensing time) and energy detection algorithms for coarse sensing (with a short sensing time).

2.2.5 Advantages

Cyclostationary detection does not require a noise power estimate. Cyclostationary detection can also be used for signal classification, as shown from research in [12].

2.2.6 Drawbacks

Cyclostationary detection is thought of as the more robust technique by many researchers since noise does not exhibit spectral correlation (SCD is zero). However this only applies to the "true" SCD which in theory involves sensing for an infinite amount of time. Practical estimates of the SCD use a finite sensing time causing the SCD estimate for noise to be small but not zero (as shown in Section 2.2.3). Increased sensing time increases performance of cyclostationary detection but also increases performance of energy detection, since more Fourier transform averages produce a flatter noise spectrum. Existing research has shown that cyclostationary feature detection requires longer sensing time to achieve the same performance as energy detection [13]. As mentioned in Section 2.2.4, some cyclostationary detection algorithms require a-priori knowledge of the signals to be detected, which is not useful for blind detection. Additionally, the entire bandwidth of a signal must be captured in order for spectral correlation to be seen. Partially captured signals may not exhibit any spectral correlation. For example, if the receiver's bandwidth only covers half of the bandwidth of a signal, spectral correlation features may be completely nonexistent in the SCD estimate. Computation of the SCD also involves higher computational complexity leading to increased use of hardware/software resources in implementation.

2.3 Detector Performance Metrics

The common metrics to characterize the performance of a signal detector are the probability of detection (P_D) and the probability of false alarm (P_{FA}). P_D is the probability of correctly detecting a signal; in other words, the probability for the system to detect a signal when in reality a signal is present. P_{FA} is the probability of incorrectly detecting a signal; in other words, the probability for the system to detect a signal when in reality no signal is present. A related metric is the required SNR for a certain P_D , which is the minimum SNR required to correctly detect a signal with probability P_D .

The value of P_{FA} depends only on the detection threshold(s) chosen.

The higher the value of P_{FA} , the more available spectrum opportunities are missed. The value of P_D depends only on the received SNR. The lower the value of P_D , the more likely it is to interfere with primary users or other secondary users. The IEEE 802.22 standard for cognitive radio networks specifies that P_{FA} should be less than or equal to 0.1 and P_D should be greater than or equal to 0.9 [2]. The two metrics oppose each other; changing the detection threshold(s) to increase P_D will also increase P_{FA} .

Another performance metric of interest is the sensing time required to meet a particular P_D and P_{FA} for a given SNR. Increasing the sensing time improves detection performance at the cost of longer idle time during which the cognitive radio cannot be transmitting. Required sensing times are desired to be as low as possible. The IEEE 802.22 standard mandates a detection time of 2 seconds or less to meet P_D and P_{FA} requirements [2].

Chapter 3

Detection Algorithm

This chapter compares single-band energy detection and cyclostationary detection algorithms for signal detection, then selects the better of the two and modifies it for multiband detection. Both considered single-band algorithms require no a-priori knowledge of the noise power, and use a simple threshold test to determine if a signal is present. The performance of both algorithms is compared through MATLAB simulations with a single signal affected by additive white Gaussian noise (AWGN). It will be seen that the energy detection algorithm yields better performance.

3.1 Single-Band Energy Detection Algorithm

The proposed single-band energy detection (ED) algorithm detects the presence of a signal using a power spectral density (PSD) estimate and does not require a-priori knowledge of the noise power. The noise power is instead estimated as the minimum value of the PSD. The basis of this estimate is the assumption that at least one frequency bin is unoccupied by signals during the sensing time. This is expected to hold true in implementations where the receiver bandwidth is large enough that typical transmissions would not occupy the entire band. The target implementation platform can receive 28 MHz of RF bandwidth, which was deemed to be wide enough to support this algorithm. This is because 28 MHz is wide enough to cover typical transmissions, including 20 MHz Wi-Fi transmissions and 6-8 MHz digital TV transmissions. Performance of this algorithm would be significantly reduced in situations where the entire observable band of frequencies is occupied by signals, as it would result in a poor noise estimate. The algorithm is described as follows:

1. Compute successive N_F -point FFTs of the input signal over time with

no windowing functions or overlap between FFTs.

$$X[k] = \sum_{n=0}^{N_F-1} x[n] \cdot e^{-j2\pi \frac{k}{N_F} n} \quad (3.1)$$

2. Compute the power spectral density (PSD) using the average squared magnitude of the FFTs.

$$S_{xx}[k] = \frac{E[|X[k]|^2]}{N_F} \quad (3.2)$$

3. Find the minimum PSD value and use it as an estimate of the noise floor.
4. Set the detection threshold Th_{ED} to be the minimum PSD value multiplied by fixed scaling factor SF .

$$Th_{ED} = \min\{S_{xx}[k]\} \cdot SF \quad (3.3)$$

5. If the maximum value of the PSD is greater or equal to Th_{ED} , assert that a signal is present.

$$\max\{S_{xx}[k]\} \geq Th_{ED} : \text{signal present} \quad (3.4)$$

The scaling factor SF is chosen based on the desired P_{FA} . Finding the SF that corresponds to a specific P_{FA} requires simulation of the detector with an input vector of pure noise; varying the SF until it produces the desired P_{FA} . Note that selection of SF does not depend on received noise power.

3.2 Single-Band Cyclostationary Detection Algorithm

The proposed single-band cyclostationary detection (CD) algorithm computes the squared magnitude of the spectral coherence and compares its maximum to a threshold to determine if a signal is present. The algorithm is described as follows:

1. Compute successive N_F -point FFTs of the input signal over time with no windowing functions or overlap between FFTs.

$$X_{N_F}[n, f] \quad (3.5)$$

2. Compute the scaled PSD using the summed squared magnitude of the FFTs. (Note: N refers to the number of successive FFTs computed).

$$\tilde{S}_{xx}[f] = \sum_{n=0}^{N-1} |X_{N_F}[n, f]|^2 \quad (3.6)$$

3. Compute spectral correlation density (SCD) by calculating the complex dot product between FFT frequency-over-time vectors at bins $(f + \alpha/2)$ and $(f - \alpha/2)$.

$$\tilde{S}_x^\alpha[f] = \sum_{n=0}^{N-1} X_{N_F}[n, f + \alpha/2] X_{N_F}^*[n, f - \alpha/2] \quad (3.7)$$

4. Compute the squared magnitude of the spectral coherence by dividing the squared magnitude of each SCD value by the product between $\text{PSD}(f + \alpha/2)$ and $\text{PSD}(f - \alpha/2)$.

$$|\tilde{C}_x^\alpha[f]|^2 = \frac{|\tilde{S}_x^\alpha[f]|^2}{\tilde{S}_{xx}[f + \alpha/2] \tilde{S}_{xx}[f - \alpha/2]} \quad (3.8)$$

5. If the maximum of the squared-magnitude spectral coherence is greater or equal to the detection threshold Th_{CD} , assert that a signal is present.

$$\max\{|\tilde{C}_x^\alpha[f]|^2\} \geq Th_{CD} : \text{signal present} \quad (3.9)$$

The detection threshold Th_{CD} is chosen based on the desired P_{FA} . Finding the Th_{CD} that corresponds to a specific P_{FA} requires simulation of the detector with an input vector of pure noise; varying the Th_{CD} until it produces the desired P_{FA} . Note that since the algorithm uses spectral coherence, the selection of Th_{CD} does not depend on received noise power.

3.3 Simulation of Single-Band Algorithms

The following simulations (performed in MATLAB) assess performance of both single-band algorithms when the input is a single baseband signal in AWGN. Single-band means that the only considered output is whether or not a signal is detected, rather than where exactly the signal is inside the band. Both QPSK and OFDM signals are tested. The simulations were performed with $N_F = 128$.

3.3.1 Setup

Two input signals are tested: a QPSK signal and an OFDM signal. Both input signals have a length of 9216 samples. Signal settings are summarized in Table 3.1. The QPSK signal is pulse shaped with a square root raised cosine with roll-off equal to 0.5. The OFDM signal contains 38 subcarriers, all of which are 16-QAM modulated at 64 samples per symbol with rectangular pulse shaping. A cyclic prefix of 8 samples is applied to each symbol to yield a total of 72 samples per symbol. AWGN is applied to both signals. Note that the signal length of 9216 samples means that 72 128-point FFTs will be computed for each algorithm.

Signal/Modulation	Setting	Value
QPSK	Number of symbols	2304
	Samples per symbol	4
	RRC roll-off	0.5
OFDM	Number of symbols	128
	Samples per symbol	72
	Number of subcarriers	38
	Subcarrier modulation	16-QAM
	IFFT size	64
	Cyclic prefix length	8 samples

Table 3.1: Setup of QPSK and OFDM Test Signals

The power spectral density and spectral coherence of the test signals in high SNR are shown in Figures 3.1 and 3.2 respectively. Plots of the QPSK signal in low SNR are also shown in Figure 3.3. The spectral coherence corresponding to $\alpha = 0$ has been omitted since it is always equal to 1. Note

that the features in the spectral coherence of the OFDM signal are much weaker than the features in the QPSK signal. Also note that in the OFDM signal, spectral correlation of the individual 16-QAM modulated subcarriers does not appear. Even with a longer signal and larger FFT size, spectral correlation in individual subcarriers is not seen; the only apparent spectral correlation is related to the outside edges of the OFDM signal. The overlap between subcarriers appears to cancel out individual spectral correlation. We also observe that the cyclostationary features of the the QPSK signal are heavily diminished in low SNR.

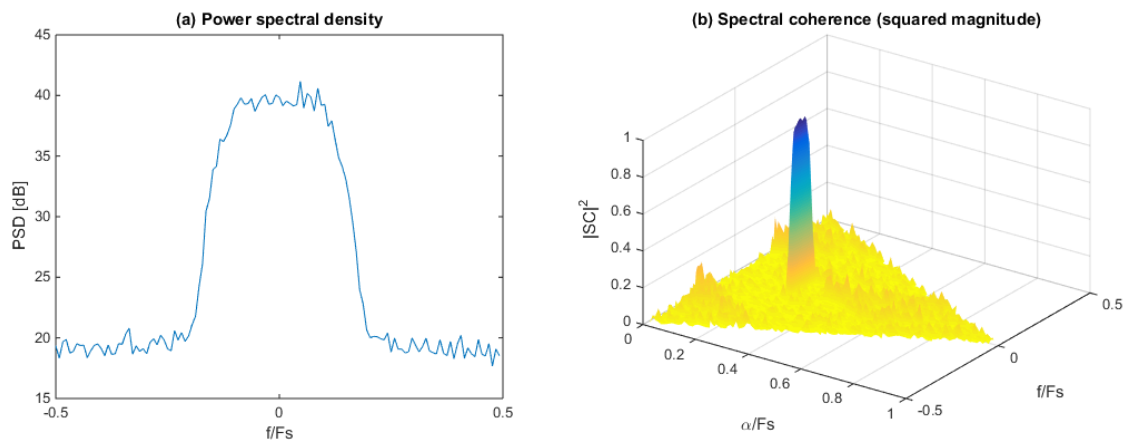


Figure 3.1: PSD and spectral coherence of 9216-sample QPSK test signal at SNR = 15dB (F_s is the sampling frequency).

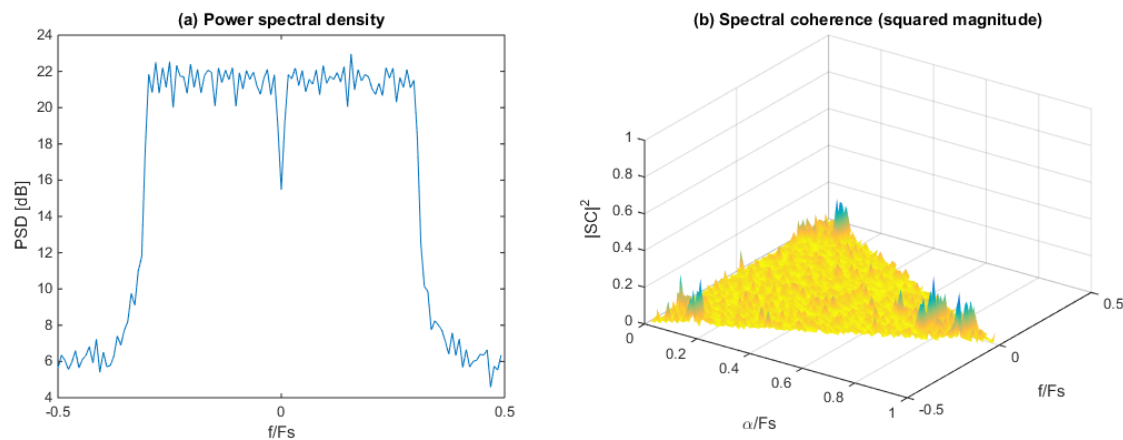


Figure 3.2: PSD and spectral coherence of 9216-sample OFDM test signal at SNR = 15dB (F_s is the sampling frequency).

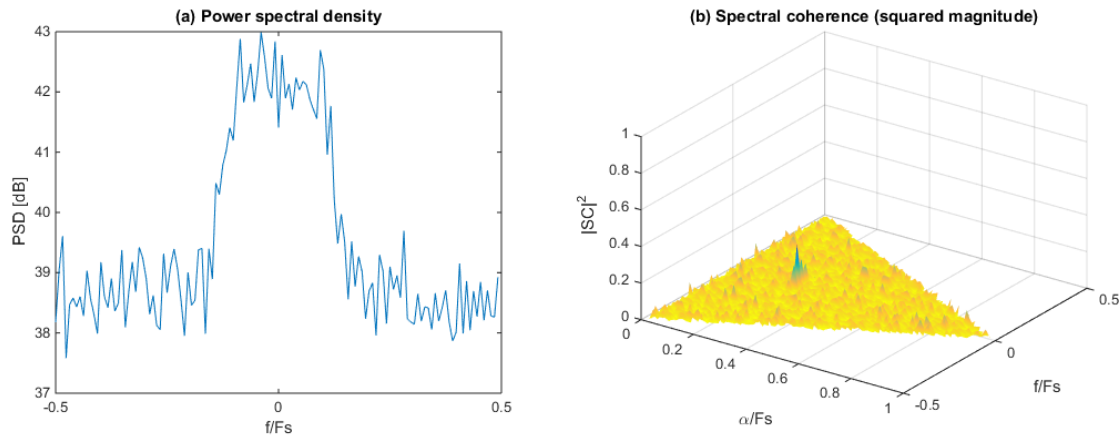


Figure 3.3: PSD and spectral coherence of 9216-sample QPSK test signal at SNR = -5dB (F_s is the sampling frequency).

3.3.2 Results

Figure 3.4 shows the resulting P_D across SNR for both test signals, with thresholds set so that $P_{FA} = 0.1$. Figure 3.5 shows the resulting receiver operating characteristic (ROC) curves with SNR held constant. The ED algorithm yields higher P_D for a given P_{FA} , for both QPSK and OFDM signals, but especially for OFDM.

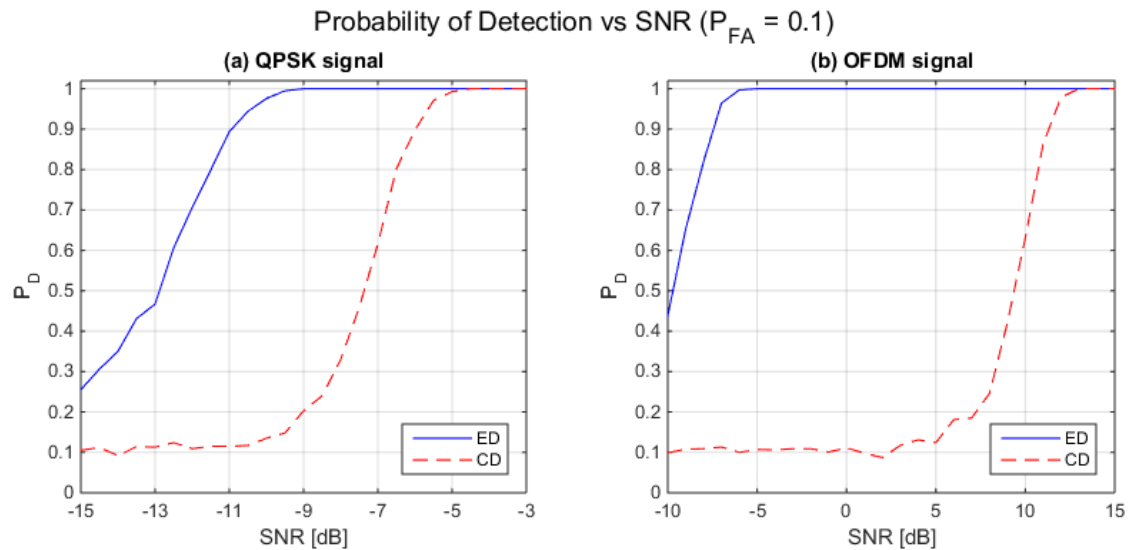


Figure 3.4: Probability of Detection vs SNR with fixed $P_{FA}=0.1$ for (a) QPSK test signal and (b) OFDM test signal.

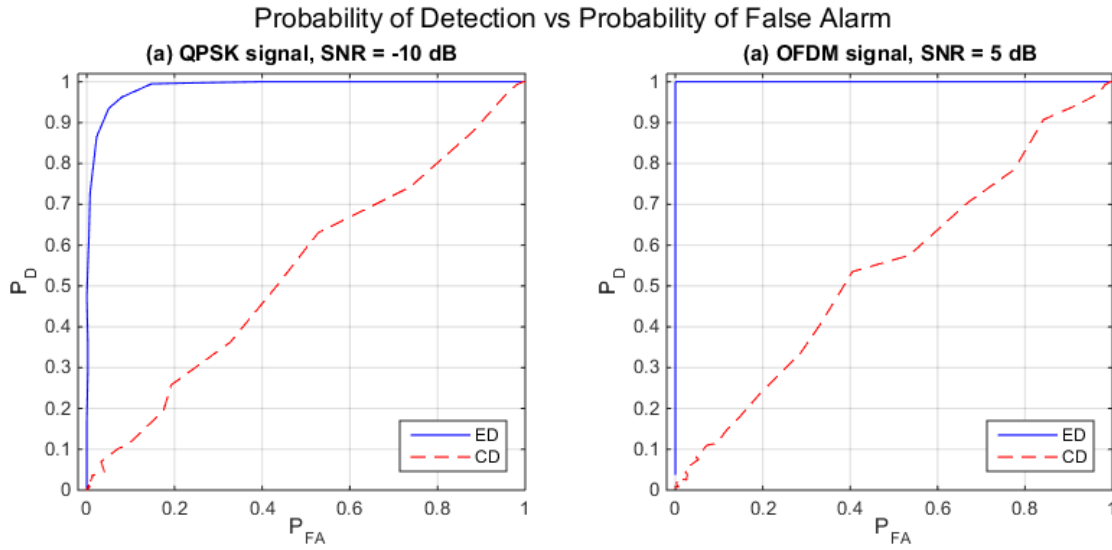


Figure 3.5: Detector ROC curves with fixed SNR for (a) QPSK test signal with SNR = -10 dB and (b) OFDM test signal with SNR = 5 dB.

Both algorithms see increases in performance when signal length is increased. In additional testing, we increased the signal length for the CD algorithm but kept the signal length the same for the ED algorithm. If signal length is increased enough for the CD algorithm, eventually it meets the performance of the ED algorithm. Specifically, we saw that increasing the signal length 6.2 times (from 9216 samples to 57344 samples) caused the curve for the CD algorithm to match the curve of the ED algorithm in Figure 3.4(a). In other words, the CD algorithm required 6.2 times the sensing time to meet the performance of the ED algorithm for detection of the QPSK signal.

3.3.3 Conclusion

The energy detection algorithm is shown to perform better than the cyclostationary detection algorithm for both QPSK and OFDM with fixed signal length. The CD algorithm needs significantly longer signal length (translating to sensing time in practice) to meet the performance of the ED algorithm. The longer sensing time makes the CD algorithm less desirable for wideband implementation, where the algorithm is applied repeatedly across

a range of frequencies to cover a very wide bandwidth. For wideband implementation the duration of a full scan may be too long to be useful for a cognitive radio. Additionally, wideband CD implementations would need to apply significant overlap between each band to sense. This is because a partially captured signal at the edge of the receiver bandwidth may not produce any features in the spectral coherence (mentioned in section 2.2.6).

The only time the energy detection algorithm may fail is when the entire band of frequencies is occupied by signals, without guard bands. In that case the value for the noise floor estimate may be so inaccurate that the algorithm will not produce expected performance. However, the target platform's 28 MHz maximum bandwidth is not expected to be entirely occupied by signals.

The simulations demonstrate the ineffectiveness of cyclostationary detection when using the maximum spectral coherence as a simple detection statistic, especially for OFDM signals. For improved cyclostationary detection in OFDM, the work in [16] suggests embedding unique cyclostationary signatures in OFDM transmissions from cognitive radios. However this may not apply to detection of primary users, who can use any type of transmission without embedded signatures.

3.4 Multiband Detection Algorithm

Based on simulation results for single-band detection, the energy detection algorithm was selected for further application. The single-band energy detection algorithm was modified to allow for detection of signals across multiple bands. The modified algorithm considers individual PSD bins instead of the maximum of all PSD bins. The modification also adds a metric to rank the strength of each spectrum hole. A higher hole ranking means the frequency bin is more likely to truly be a hole. The multiband algorithm is described as follows:

1. Compute successive N_F -point FFTs of the input signal over time with

no windowing functions or overlap between FFTs.

$$X[k] = \sum_{n=0}^{N_F-1} x[n] \cdot e^{-j2\pi \frac{k}{N_F} n} \quad (3.10)$$

2. Compute the power spectral density (PSD) using the average squared magnitude of the FFTs.

$$S_{xx}[k] = \frac{E[|X[k]|^2]}{N_F} \quad (3.11)$$

3. Find the minimum PSD value and use it as an estimate of the noise floor.
4. Set the detection threshold Th_{ED} to be the minimum PSD value multiplied by fixed scaling factor SF .

$$Th_{ED} = \min\{S_{xx}[k]\} \cdot SF \quad (3.12)$$

5. For every frequency bin with $PSD \geq Th_{ED}$, assert that a signal is present in the band corresponding to that frequency bin.

$$S_{xx}[k] \geq Th_{ED} : \text{signal present in frequency bin } k \quad (3.13)$$

6. For each frequency bin that is a hole (meaning $PSD < Th_{ED}$), divide Th_{ED} by the bin's PSD value to produce the hole ranking metric.

$$\text{Hole rank}[k] = \frac{Th_{ED}}{S_{xx}[k]} \quad (3.14)$$

Note that P_{FA} is now defined on a per-bin basis, meaning P_{FA} is the probability for an individual bin to be detected as a signal when no signal is present. Thus, when the input is pure noise, the average number of frequency bins incorrectly detected as signals is $N_F \cdot P_{FA}$.

3.5 Simulation of Multiband Algorithm

The same QPSK and OFDM test signals used in the single-band simulation (shown in Figures 3.1 and 3.2) were used to test the multiband algorithm with AWGN. Also as in the single-band simulation, an FFT size of $N_F=128$ was used. Two performance metrics were used to assess the multiband algorithm. The first metric is the average percentage of signal power detected in a signal's bandwidth. The second metric is the probability to detect at least 90% of the power in a signal's bandwidth ($P_{D,90}$). We define the signal's bandwidth as the range of frequencies around the center frequency which contain 99.5% of the signal's power. We test these performance metrics against different levels of in-band SNR; defined as the ratio of signal power to noise power inside the signal's bandwidth.

3.5.1 Results

Figure 3.6a shows the average percent of signal power detected in the signal's bandwidth across in-band SNR. Figure 3.6b shows the resulting probability of detecting 90% of the power in the signal's bandwidth across in-band SNR. Thresholds corresponding to a P_{FA} of 0.1 and 0.01 were used. Slightly worse performance is seen from the OFDM signal at lower SNRs. This may be caused by the wider bandwidth of the OFDM signal (74% of the sampling bandwidth) vs the QPSK signal (35% of the sampling bandwidth). The wider bandwidth leaves fewer free bands for the algorithm's noise floor estimate. Fewer free bands means that the estimate of the noise floor will be higher, resulting in a higher detection threshold. A higher detection threshold results in a lower probability of detection.

Figure 3.7 illustrates the effects of varying algorithm parameters (but keeping P_{FA} the same) on detection performance for the QPSK test signal. Figure 3.7a shows the performance gain from increasing the signal length from 9216 to 32768, thereby increasing number of FFT averages from 72 to 256. The trade-off is an increased sensing time. Figure 3.7b illustrates the performance gain from decreasing the FFT size from 128 to 64. Performance increases because (1) the increased bandwidth of each FFT bin

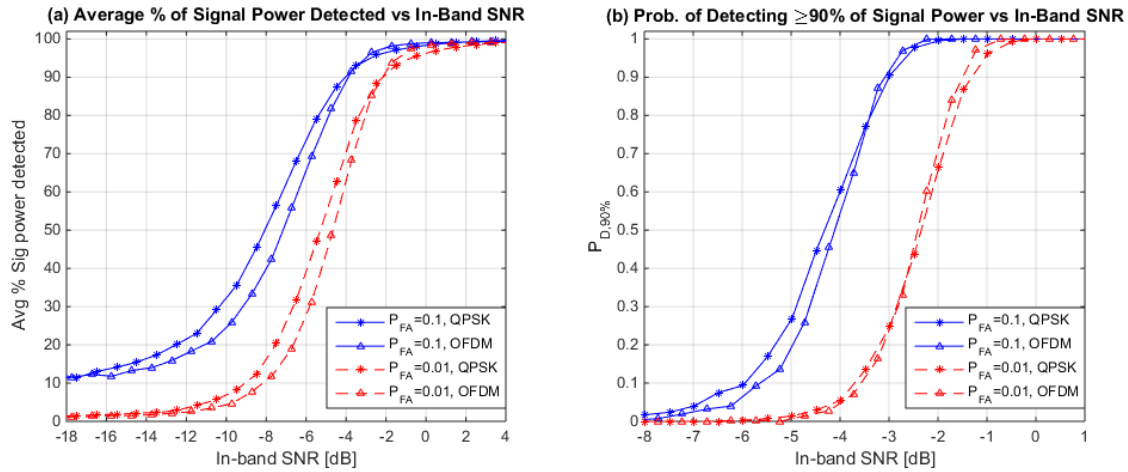


Figure 3.6: Performance of multiband energy detection algorithm. (a) Average percentage of signal power detected in signal's bandwidth vs in-band SNR (b) Probability of detecting at least 90% of the power in signal's bandwidth vs in-band SNR

naturally smooths each FFT and (2) more successive FFTs will be averaged. The trade-off is a decrease in the frequency resolution of the detector.

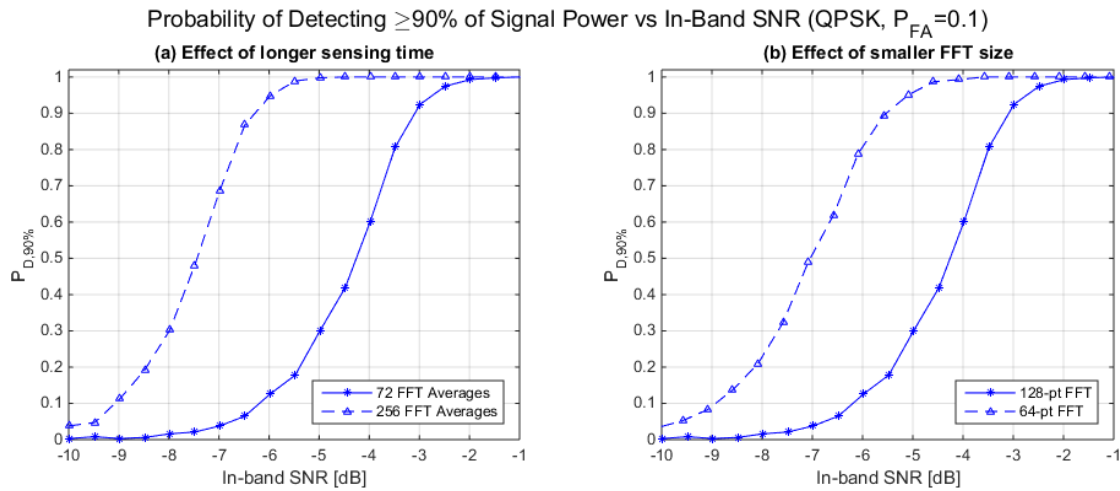


Figure 3.7: Effects on detection performance (a) increased sensing time (and therefore number of FFT averages) and (b) decreased FFT size.

3.5.2 Remarks for Implementation

We note that false alarms in the multiband algorithm can be more troublesome for cognitive radios. Sparse false alarms cut into wide bands of

continuous holes, causing there to be a lack of reported holes with wide bandwidths. A lower probability of false alarm may be desired if wider hole bandwidths are needed for communication. For the best detection performance, sensing time should be increased as much as possible since it adds more FFT averages. As mentioned in Section 3.5.1, a longer sensing time yields significant increases in detection probability. FFT size should be chosen as the smallest size that satisfies requirements for frequency resolution of the detector. As mentioned in Section 3.5.1, a smaller FFT size also significantly increases detection probability.

Chapter 4

Implementation

4.1 SDR Platform

The implementation platform is the bladeRF x115 USB 3.0 software-defined radio, produced by Nuand LLC. The bladeRF can tune from 0.3 GHz to 3.8 GHz and can transmit/receive 28 MHz of instantaneous bandwidth with a 40 Msps sampling rate and 12-bit sampling resolution. The bladeRF contains an Altera Cyclone IV E FPGA with 115k logic elements which sits between a Lime Micro LMS6002D field-programmable RF transceiver and a Cypress FX3 USB 3.0 controller. The board interfaces with a host PC through its USB 3.0 port. The board's FPGA allows signal processing to be performed in hardware in addition to software on the host PC. The default FPGA bitstream contains an Altera Nios II soft processor for command and control (setting the frequency, gains, etc.) and a datapath to transfer IQ samples to/from the FX3 chip. The soft processor interfaces with the FX3 via UART and interfaces with the LMS6002D through SPI. The datapath interfaces with the FX3 via GPIF II and interfaces with the LMS6002D's DACs/ADCs via a direct simple protocol. Figure 4.1 shows a block diagram of the implementation platform. The TX chain in the RF front end is unused in the implementation and was therefore omitted from the diagram.

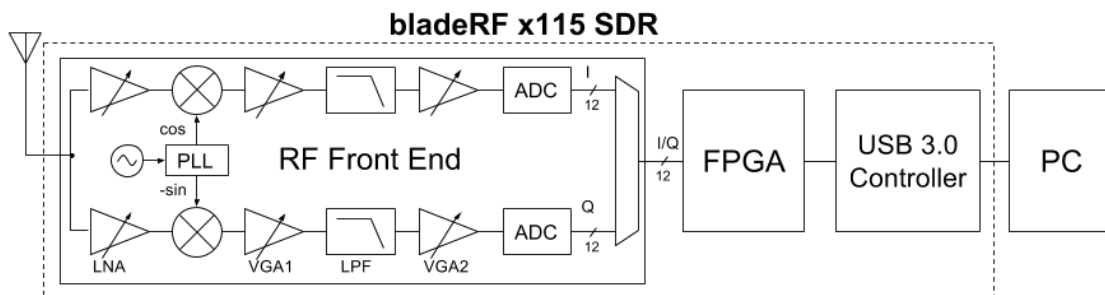


Figure 4.1: Block diagram of receive chain in the bladeRF implementation platform

Figure 4.2 shows a photograph of the actual bladeRF device, with USB cable plugged in and antennas attached to the transmit and receive ports.

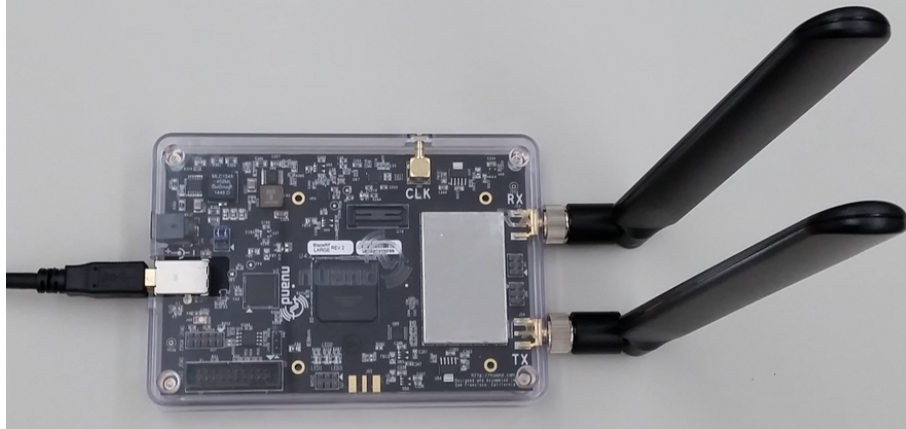


Figure 4.2: Image of bladeRF device

4.2 Implementation Overview

The detector implementation applies the proposed multiband energy detection algorithm to cover a wide bandwidth for cognitive radio applications. Although the bladeRF can only receive 28 MHz of instantaneous bandwidth, the implementation scans GHz ranges by repeatedly changing the receive frequency and performing the multiband energy detection algorithm at each frequency. Figure 4.3 illustrates the the detector's method of operation over a wide bandwidth.

The frequencies to scan are software-configurable; the maximum number of frequencies is 125 which can cover the bladeRF's entire 0.3 GHz - 3.8 GHz range. The larger the frequency range, the more time each full scan requires. We refer to the full scan time as the latency. This latency represents the total sensing and processing time for each full scan. The latency of a full scan (t_{scan}) is equal to the number of frequencies (N_{freq}) multiplied by the sum of the sensing time per band ($t_{sense,band}$) and the retune time (t_{retune}), shown in equation 4.1. Additional delay at the end of a full scan due to pipelining in the FPGA is negligible and has been omitted from the

calculation.

$$t_{scan} = (t_{sense,band} + t_{retune}) \cdot N_{freq} \quad (4.1)$$

For covering the bladeRF's entire 3.5 GHz range, the latency of each full scan is roughly 169 ms. Retune time is not instant, since it involves adjusting parameters of the RF front end's phase-locked loop to guarantee lock via SPI transactions. The implementation's retune time was determined to be $532.9 \mu s$ (see Section 5.3.1) and the sensing time per band is $819.2 \mu s$. The sensing time per band refers to the amount of time spent receiving samples for an individual 28 MHz band, and is determined by the sampling rate and number of samples received per band. The implementation detects holes with a resolution of 314.6 kHz.

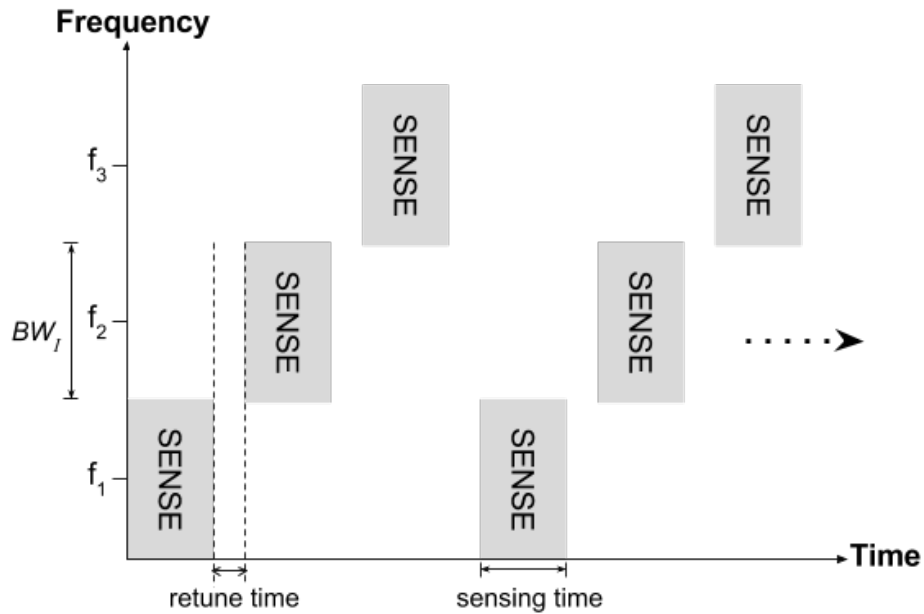


Figure 4.3: Method of operation for scanning wide bandwidth: example with 3 frequencies. Illustrates the sensing time (per band), retune time, and instantaneous bandwidth of the receiver BW_I

4.3 Implementation Architecture

The implementation performs all processing on the FPGA. Figure 4.4 shows a diagram of the detector architecture. The architecture consists of a software program (running on the Nios II soft processor) for frequency tuning and control, and a hardware datapath for signal processing and hole detection. Receiver amplifier gains in the RF front end were set to constant values rather than different values based on frequency. No automatic gain control was used. Implementation specifications and settings are summarized in Table 4.1.

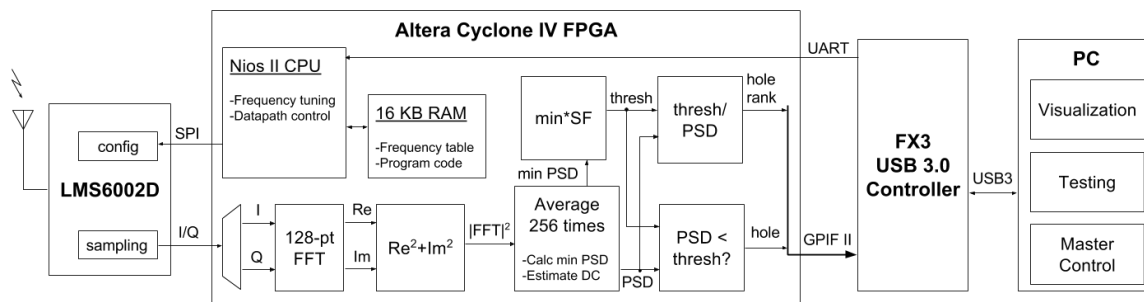


Figure 4.4: Implementation Architecture

Specification/Setting	Value
IQ sampling rate	40 Msps
Instantaneous bandwidth	28 MHz
FFT size	128 ¹
Frequency resolution	314.6 kHz
IQ samples per band	32768
Sensing time per band	819.2 μ s
Number of FFT averages per band	256

Table 4.1: Implementation Specifications and Settings

¹After computing each FFT, the number of FFT bins is clipped from 128 to 89 (see Section 4.3.1)

4.3.1 Hardware datapath

The hardware datapath refers to all blocks inside the FPGA in Figure 4.4 besides the Nios CPU and 16 KB RAM. For each frequency, the hardware datapath receives 32768 IQ samples at 40 Msps (for a sensing time of 819.2 μ s) and performs successive 128-point FFTs. Although the 40 Msps sampling rate produces a received bandwidth of 40 MHz (-20 MHz to +20 MHz), the lowpass filter in the RF front end reduces the passband bandwidth to 28 MHz (-14 MHz to +14 MHz). The FFT frequency bins outside of the 28 MHz lowpass filter bandwidth are discarded, reducing the number of frequency bins from 128 to 89. The signal is oversampled at 40 Msps to reduce aliasing. The squared magnitude of the FFT results are averaged to produce a PSD estimate. Each PSD estimate uses 256 FFT results for averaging. The minimum value of this PSD estimate is multiplied by a fixed scaling factor to produce the detection threshold. Frequency bins which contain PSD values less than the threshold are deemed spectrum holes. Spectrum holes are ranked by the division of the threshold value by the individual PSD value.

4.3.2 Nios software

The Nios program cycles through a frequency table stored in attached embedded RAM and tunes the RF front end to each frequency via SPI. Once tuning to a certain frequency is complete, the program asserts a control register bit which tells the hardware datapath to receive samples. Once 32768 samples have been received the datapath interrupts the Nios CPU, after which the Nios program tunes to the next frequency and repeats.

4.3.3 PC interface

The PC software interface allows for master control and reception of detector output samples so that experiments can be run. The PC software communicates with the Nios program to configure gains, bandwidth, sampling rate, and other settings before the detector is enabled. Receive amplifier gains were set to constant values, rather than different values based on frequency. The PC software also generates the frequency table which is sent

to the Nios program for storage in its RAM. To enable the detector the PC software sends a 'start' packet to the Nios program, after which the detector begins continuously scanning; repeating until the PC software sends a 'stop' packet. The detector outputs one 32-bit sample for each frequency bin. The output sample consists of a single 'hole' bit (1=hole, 0=signal), a 7-bit hole ranking, and a 24-bit PSD value for visualization purposes.

4.4 Details

4.4.1 Design

The FPGA logic was designed with VHDL. Two Altera Intellectual Property (IP) cores were used as part of the design: the 128-point FFT and a pipelined divider for calculating the hole ranking. The datapath processes samples in pipelined fashion, meaning that the outputs of one module are fed serially into the next module; with one sample per clock cycle. The serial transfer of samples allowed the datapath to be very efficient in hardware resources, since multiple parallel clones of the same hardware block were not needed. In order to sample at 40 Msps, the FPGA clock rate was set to 80 MHz (it must be double the sampling rate to acquire both the I and Q samples from the LMS6002D). Additionally, the Nios CPU ran at a clock rate of 80 MHz. Both the Nios software and the PC software for receiving detector output samples were written in C. A program for real-time visualization of PSD and holes was written in MATLAB.

4.4.2 DC Offset Handling

Direct conversion receivers suffer from unwanted baseband DC offset due to imperfections in the analog signal chain. This manifests itself as a large spike in the middle of the spectrum and must be removed. Instead of compensating for DC offset, the detector estimates the PSD value of the DC bin with the average of PSD values at the two adjacent bins. Initially, the implementation used a precomputed DC offset lookup table stored inside the FPGA with DC offsets for each corresponding frequency. Each DC offset

value was computed by receiving a large number of samples and recording the average I value and average Q value. The FPGA would subtract the DC offset from the received IQ signal on the fly. However, this proved to be ineffective, as the DC offset tended to quickly change over time causing the spike to still be seen at unacceptable levels. Methods of analog correction in the LMS6002D also proved to not be precise enough to completely remove the DC spike in the spectrum. Thus the DC PSD value was ignored and estimated using adjacent bins. Other implementations may require dynamic DC offset cancellation if the true PSD value of the DC bin is desired.

4.4.3 Fixed-point Bit Growth

Fixed-point arithmetic causes large bit growth; especially in multiplications. When results are rounded or truncated to reduce bit growth, precision loss occurs. In order to reduce this, the implementation performs minimal bit reduction in the FPGA. 12-bit I and Q input samples are passed to the FFT block which outputs 12-bit real and imaginary parts of the FFT along with a scaling exponent. After power calculation and application of the scaling exponent (not shown in Figure 4.4), the squared magnitude FFT samples are 39-bits long. The averaging block computes the sum of 256 39-bit samples, requiring 47 bits for each sum, then removes the 8 least significant bits to divide by 256 and output a 39-bit average (PSD). The minimum PSD value along with DC estimation are computed on the fly. The scale factor is stored in a 13-bit Q1.12 number. The threshold is computed by multiplication with the scaling factor followed by removal of the fractional bits.

4.4.4 Antenna and Frequency Considerations

The energy detection algorithm performed at each frequency depends on the fact that the signal gain is flat across the entire 28 MHz band. However, at certain bands which are at the edges of antenna frequency ranges, the signal gain may change sharply across the band. Performance of the algorithm will be negatively affected in these areas; one side of the band may automatically be classified as a signal since its PSD level is higher than the other side. This may cause extra false alarms, reducing the performance of the

detector. Therefore, the detector should not be applied to frequency bands where the antenna gain is not flat across the entire band. The implementation can still work at frequency ranges in which the antenna has low gain, as long as the gain is flat across each 28 MHz band. However, the reduced SNR may significantly reduce the probability of detection. Dipole antennas with a frequency range of 698-2700 MHz were used for testing of the implementation with real-world signals.

4.5 Resource Utilization

The reported FPGA resource utilization accounts only for the hole detector hardware. This includes the datapath hardware, Nios system hardware related to the hole detector (CPU, RAM, and interface peripherals), and hardware for interfacing with the RF front end. Other logic, including unused logic (i.e. the TX path) and logic used to transfer output samples to the PC through the FX3 chip, is not considered. Resource utilization is summarized in Table 4.2. The detector used an average of 8.8% of available resources on the Altera Cyclone IV E FPGA.

Resource	Usage			Percentage of FPGA
	Datapath	Nios + Interfaces	Total	
4-input LUT	10680	1391	12071	10.5%
1-bit Register	9265	934	10199	8.9%
18x18 Multiplier	17	0	17	6.4%
8 Kb Memory Block	22	19	41	9.5%

Table 4.2: FPGA Resource Utilization of Hole Detector

4.6 Requirements for Implementation

This section summarizes the critical hardware needed to implement the proposed spectrum hole detector. In addition to the digital hardware resources reported in Table 4.2, a crucial requirement of the implementation is a field

programmable RF front end that can quickly change its local oscillator frequency over a wide range. Without dynamic retuning, the wide range of frequencies needed by cognitive radios cannot be sensed. As mentioned in section 3.1, the implemented energy detection algorithm only performs well if the received bandwidth at each frequency is not completely occupied by signals. Therefore a fairly wide instantaneous bandwidth is needed for the implementation. Given that typical real-world transmissions are 20 MHz or less in bandwidth, we recommend an instantaneous bandwidth greater than 25 MHz for low probability that the entire band is occupied by signals. If wider bandwidth signals are expected, a higher instantaneous bandwidth is required for good performance from the algorithm.

4.7 Source Code

Implementation source code, including both VHDL hardware description and C software, has been provided online at:

<https://github.com/ifrasch/bladeRF-shd>

Chapter 5

Experiments and Results

After finalizing the detector implementation, experiments were performed on the detector to assess its performance and uncover any implementation issues. Performance experiments were performed using wired channels. This chapter discusses implementation issues, experimental setup, and experimental outcomes.

5.1 Implementation Issues

Testing revealed some issues related to the analog nature of the RF front end.

5.1.1 Spurious Tones in Noise Spectrum

When running the detector with no antenna on the receiver (only noise), we noted that spurious tones showed up at certain frequencies in the received power spectral density. These tones were separate from the expected DC offset spikes at each frequency. The tones showed up as small spikes 5-15 dB above the noise floor. 1-2 tones were seen for every 28 MHz band of frequencies received. We verified that tones continued to show up even after running RF front end calibration routines, and receiving samples with the default FPGA image instead of the hole detector image. This issue was also seen in the work in [17]. The origin of the tones is unknown, but is expected to be imperfections in the analog circuitry in or around the RF front end. We noted that after attaching an antenna, the number of visible tones decreased drastically as they were overwhelmed by background noise picked up by the antenna. The tones have the effect of increasing the probability of false alarm of the detector implementation. Each tone is usually detected as a signal, adding to the number of false alarms.

5.1.2 Analog Filter Frequency Response

Testing of the detector also revealed an issue with the lowpass filter inside the RF front end. The frequency response of the lowpass filter is not flat inside the passband. The magnitude of the frequency response is lower around DC and higher around the cutoff frequency. Specifically, the magnitude is around 1 dB higher at the cutoff frequency than at DC. This issue was also noted in the work in [17]. This issue caused extra false alarms to be seen around the lower and upper ends of each 28 MHz frequency band (at baseband, the lower end corresponds to -14 MHz, and the upper end corresponds to +14 MHz). When running the detector with a scaling factor produced by MATLAB simulations for $P_{FA}=0.1$, an actual P_{FA} of 0.4 was seen. The detector's scaling factor had to be increased to reach $P_{FA}=0.1$. The end result is that a higher detection probability is seen for frequencies near the cutoff frequency, and a lower detection probability is seen for frequencies around DC.

We identified a solution to this issue but did not have time to add the solution to the implementation. Although the shape of the filter response is not flat in the passband, it is consistent. Compensating for the shape of the filter response in the implementation would remove its unwanted effects. Compensation must be applied to the PSD values directly before the minimum PSD is calculated and before any hole detection. Compensation values can be applied as a set of precomputed scaling factors stored in a read-only memory. The appropriate scaling factor would be selected based on the frequency index of the PSD value to scale.

5.2 Side Experiment: Noise Characterization

5.2.1 Noise Floor Variation

A side experiment was done to confirm the problem of varying noise levels for noise power estimation, a problem mentioned as a drawback to energy detection in Chapter 2. The bladeRF platform with stock FPGA image was used to scan the 0.3-3.8 GHz spectrum. Gqrx SDR software was used to view the spectrum and tune to different frequencies with the bladeRF. With

the receive antenna unattached and replaced with a 50-ohm terminator, internal noise power from the RF front end varied by 20 dB between the lowest frequency (0.3 GHz) and the highest frequency (3.8 GHz). Simply attaching the antenna increased the observed noise power by 10-15 dB at certain frequency bands. Adjusting the orientation of the antenna also changed the observed noise power by 10-15 dB at certain frequencies. This confirms that a static estimate of the noise floor is not possible for energy detection. A dynamic estimation technique, like the one used in the proposed algorithm, is needed for energy detection on realistic systems.

5.2.2 PSD and Spectral Coherence of Noise

We examined the PSD and spectral coherence of noise generated from the RF front end in order to compare it to simulated white Gaussian noise. The bladeRF with stock FPGA was used to receive 32768 samples at 40 Msps, with the low pass filter of the RF front end set to 28 MHz and a 50-ohm terminator attached to the receive port. The frequency was set to 1254 MHz. MATLAB software was used to compute successive 128-point FFTs of the received signal. As in the detector implementation, FFT bins outside of the 28 MHz filter bandwidth were discarded. We computed the PSD and spectral coherence using the same techniques as in the simulations in Chapter 3. As in implementation, the PSD of the DC bin was estimated using the mean PSD of the adjacent bins. Figure 5.1 shows the resulting PSD and spectral coherence estimates of the noise.

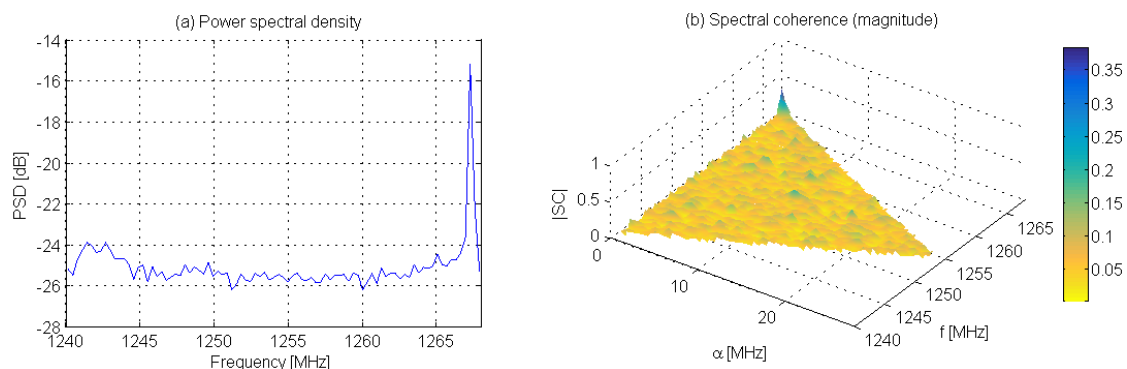


Figure 5.1: PSD and spectral coherence estimates of real noise received with the bladeRF

The non-flat shape of the PSD from the lowpass filter issue discussed in Section 5.1.2 is clearly seen. One spurious tone (issue discussed in Section 5.1.1) is also seen in the PSD plot at a frequency of 1267 MHz. The spectral coherence of the noise is mostly flat with a mean magnitude of around 0.1. Unexpectedly, the spurious tone produces a small peak in the spectral coherence magnitude equal 0.37 to at $(f, \alpha) = (1267 \text{ MHz}, 0.63 \text{ MHz})$. The spurious tone produces more spectral correlation than the surrounding white noise. This means that spurious tones could also cause false alarm issues in cyclostationary detection algorithms.

5.3 Setup of Performance Experiments

Figure 5.2 illustrates the experimental setup. The setup consisted of three bladeRF SDR devices transmitting through SMA cables to one receiver bladeRF performing hole detection. The three transmitted signals were added using a 4:1 RF combiner. After the combiner, two 30 dB attenuators were applied to protect the receiving device and reduce SNR. All bladeRF devices were connected through USB 3.0 to a PC.

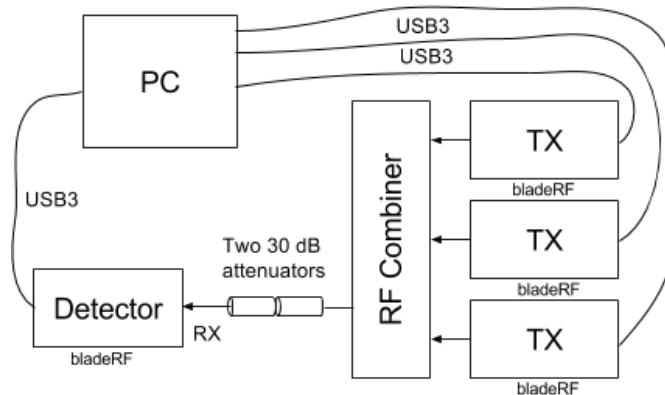


Figure 5.2: Experimental Setup

The same QPSK and OFDM test signals from Section 3.3.1 (simulation setup) were used for testing the detector, with the number of symbols increased to yield longer signals. The number of symbols in the QPSK signal was increased to 16384 for a signal length of 65536 samples. For transmission of the QPSK signal using the bladeRF SDR, a sampling rate of 15

Msp/s was used, resulting in a signal bandwidth of 5 MHz. The bandwidth of the lowpass filter in the transmit chain of the RF front end was set to 12 MHz. The number of symbols in the OFDM signal was increased to 896 for a signal length of 64512 samples. For transmission of the OFDM signal, a sampling rate of 24 Msp/s was used, resulting in a signal bandwidth of 16.5 MHz. The bandwidth of the lowpass filter in the transmit chain of the RF front end was set to 20 MHz. Each signal transmission was repeated indefinitely to result in a continuous transmission.

5.3.1 Detector Parameters and Characteristics

The detector parameters used for performance experiments as well as latency characteristics are summarized in Table 5.1. The detector's frequency table was configured to scan frequencies from 1308 MHz to 2288 MHz for a total sensing bandwidth of 980 MHz. This configuration involves 35 frequency retune operations for each full scan of the detector. The scaling factor for the detector implementation was set to 1.455, producing a measured P_{FA} of 0.09. P_{FA} was measured by running the detector with a 50-ohm terminator on its receive port, and counting the number of false alarms across all frequencies; repeating for 500 iterations. As noted in Section 5.1.2, imperfections in the lowpass filter inside the RF front end caused the scaling factor for implementation to differ from the expected scaling factor from simulation.

Parameter/Characteristic	Value
Scaling factor	1.455
P_{FA}	0.09
Number of frequencies	35
Frequency range	1308 - 2288 MHz
Total bandwidth	980 MHz
Retune time	532.9 μ s
Full scan time	47.3 ms

Table 5.1: Detector Parameters and Characteristics

Software was used to measure the time between reception of each full 980 MHz scan from the detector. We found that the latency of each full

scan was 47.3 ms. Dividing the total latency by the number of frequencies (35) and subtracting the chosen sensing time per band ($819.2 \mu\text{s}$) yields an average retune time of $532.9 \mu\text{s}$.

5.4 Results

5.4.1 Single Transmission

This experiment was performed with a single transmission from one bladeRF device. To eliminate bias from the analog filter issue discussed in Section 5.1.2, two different carrier frequencies were used. One carrier frequency was placed at the center of one of the detector's frequency bands, and the other carrier frequency was placed at the edge of one of the detector's frequency bands. The carrier frequencies used were 2134 MHz and 2148 MHz.

The performance metric tested was the probability of detecting at least 90% of the power in the signal's bandwidth ($P_{D,90}$). As mentioned in Section 3.5 (simulation of multiband algorithm), we define the signal's bandwidth as the range of frequencies around the center frequency which contain 99.5% of the signal's power. For each test signal (QPSK and OFDM), the detection probability results from the two carrier frequencies used were averaged to produced a final number for $P_{D,90}$.

Figure 5.3 shows the resulting $P_{D,90}$ of the detector across in-band SNR for both the QPSK signal and the OFDM. We see that for a given in-band SNR, $P_{D,90}$ is higher for the QPSK signal than for the OFDM signal. As mentioned in Section 3.5.1 (multiband simulation results), we speculate that the reason for worse performance with the OFDM signal is the wider bandwidth of the signal (16.5 MHz) in comparison to QPSK signal (5 MHz). The wider bandwidth leaves fewer unoccupied frequencies inside the detector's instantaneous bandwidth (28 MHz), resulting in a higher estimate for the noise floor. This higher estimate of the noise floor results in a higher detection threshold, yielding a lower probability of detection. Figure 5.4 shows the resulting receiver operating characteristic (ROC) curve of the detector with in-band SNR fixed at -6 dB. The ROC curve was generated by varying the detector's scaling factor and measuring each corresponding $P_{D,90}$ and

P_{FA} value.

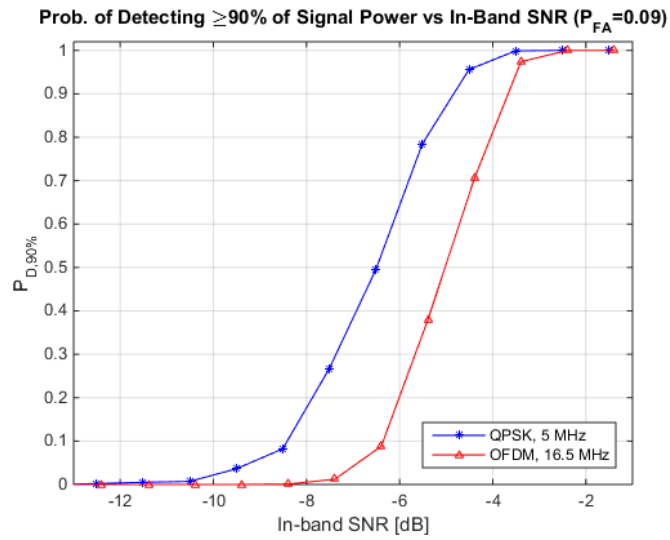


Figure 5.3: Detector performance for a single continuous transmission and fixed $P_{FA} = 0.09$

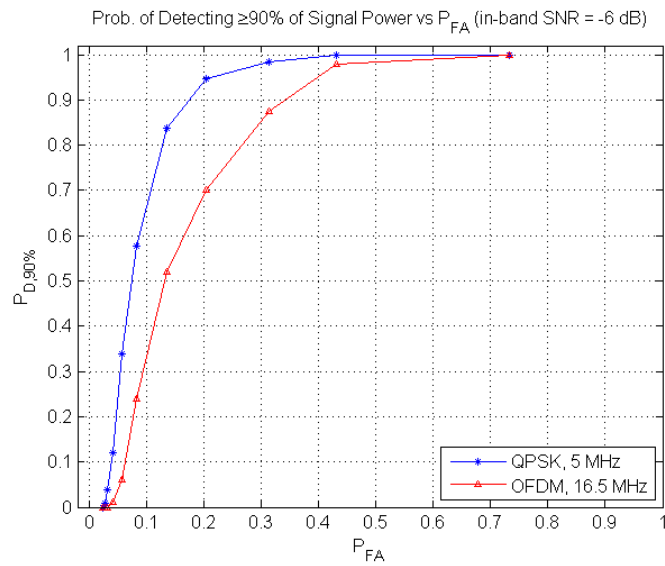


Figure 5.4: Detector ROC curve for a single continuous transmission and fixed in-band SNR = -6 dB

5.4.2 Multiple Transmissions

This experiment was performed with three continuous transmissions from three bladeRF devices. The three frequencies used were 1443.4 MHz, 1648.6 MHz, and 2111.7 MHz. Tests for QPSK signals and OFDM signals were kept separate. The transmit gain of each transmission was adjusted so that all transmissions had the same in-band SNR (± 0.5 dB). The gains were then increased or decreased together in order to vary in-band SNR.

The performance metric tested was the probability of detecting at least 90% of the power in every signal ($P_{D,90}^{all}$). Essentially, this is the probability to detect all signals at any given time. Figure 5.5 shows the resulting $P_{D,90}^{all}$ across in-band SNR, for both QPSK transmissions and OFDM transmissions. Interestingly, the performance of the detector with the OFDM signals is about the same as the performance with the QPSK signals.

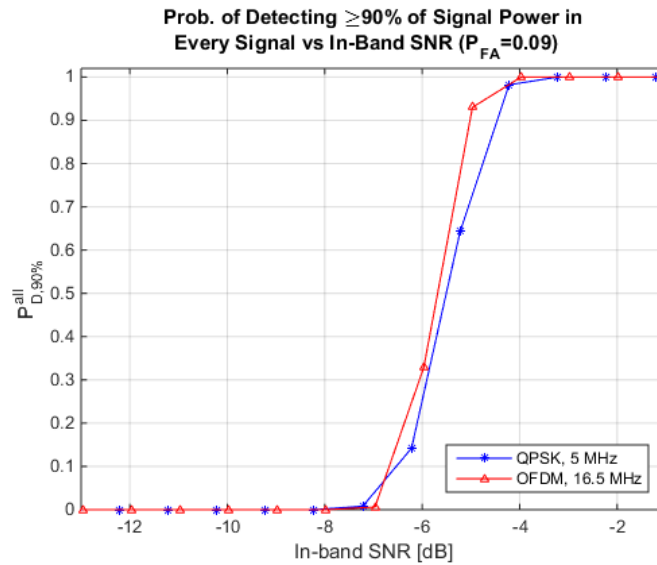


Figure 5.5: Detector performance for three continuous transmissions

5.4.3 Example Detector Output

Figure 5.6 shows an example of a portion of the detector's real-time output in the presence of three wired QPSK transmissions at 1420 MHz, 1443 MHz, and 1488 MHz. Each QPSK signal has an in-band SNR of -2 dB.

The frequency range of the output plots has been restricted to a small 112 MHz window. The vertical dotted lines show the boundaries between each 28 MHz band of the detector. In the hole detection plot (Figure 5.6(b)) the shaded areas are detected holes. Note the presence of unwanted spikes in the power spectral density due to the tones discussed in Section 5.1.1. Also note that the false alarms seen in the holes plot are expected because the detector was designed for a P_{FA} of 0.09. The detector successfully identifies spectrum holes and classifies the three signals as non-holes.

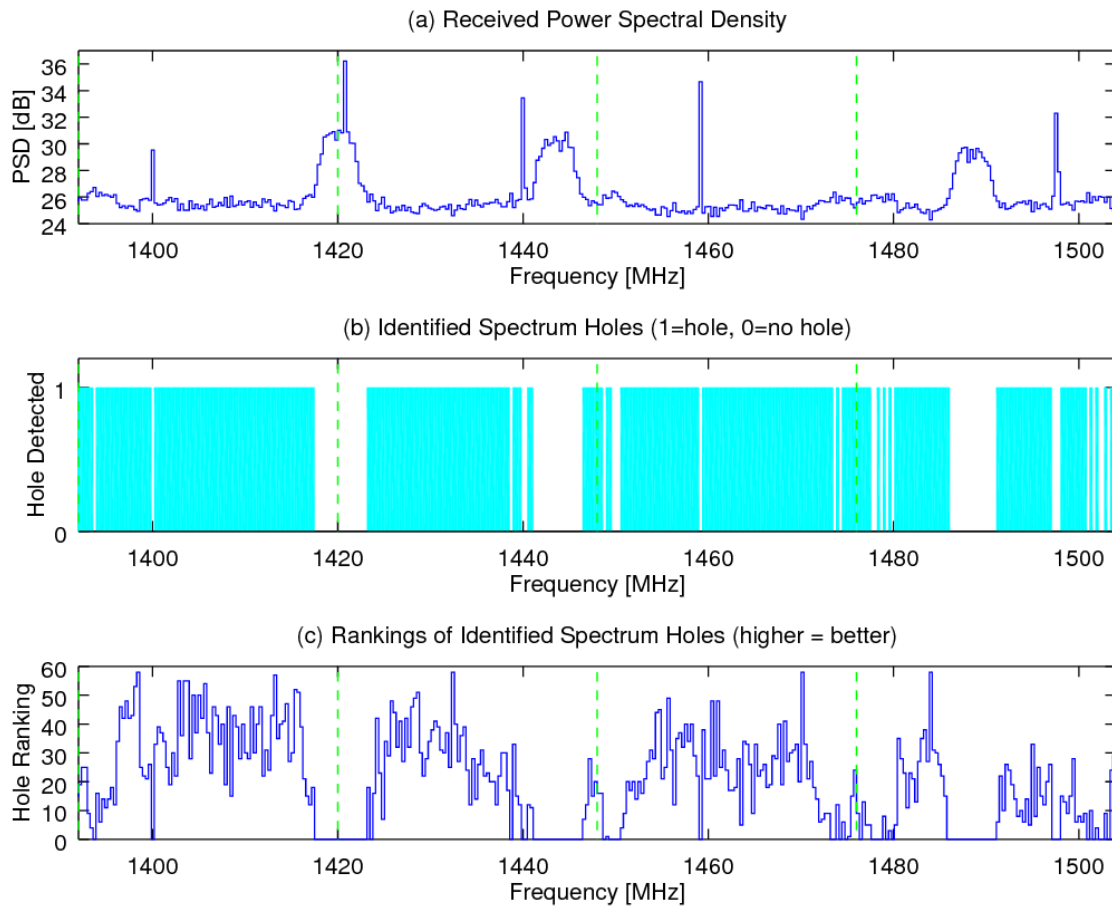


Figure 5.6: Real-time output from the detector with three wired QPSK transmissions with bandwidths of 5 MHz. (a) Scaled power spectral density; (b) Detected holes; (c) Rankings of detected holes.

Chapter 6

Conclusion

This research consisted of the design, simulation, implementation, and analysis of a spectrum holes detector for cognitive radio applications. Single-band cyclostationary detection and energy detection algorithms which do not require a-priori knowledge of noise power were compared and analyzed. Simulations concluded that the performance of the energy detection algorithm was significantly higher than the performance of the cyclostationary algorithm. The energy detection algorithm produced a higher P_D for a given P_{FA} and fixed sensing time. A multiband energy detection algorithm suitable for wideband implementation was proposed. The open-source SDR implementation demonstrated efficient application of the algorithm for an extremely wide bandwidth, with reasonable latency, suitable for usage in cognitive radios. Implementation issues and hardware/resource requirements were described in detail.

This work contributes to a better understanding of implementation feasibility of spectrum hole detection for cognitive radios. Future work includes system design for cooperative spectrum sensing with multiple radios as well as signal classification using spectral coherence.

Bibliography

- [1] Molisch, Andreas F, *Wireless Communications, Second Edition*. John Wiley and Sons, Ltd, 2011, page 506.
- [2] I. S. Association, “Cognitive Wireless RAN Medium Access Control and Physical Layer Specifications: Policies and Procedures for Operation in TV bands,” *IEEE Standard 802.22-2011*, p. 447, Jun. 2011.
- [3] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb 2005.
- [4] Federal Communications Commission. White Space Database Administration. Accessed 2017-04-19. [Online]. Available: <https://www.fcc.gov/general/white-space-database-administration>
- [5] D. Cabric, S. M. Mishra, and R. W. Brodersen, “Implementation issues in spectrum sensing for cognitive radios,” in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, Nov 2004, pp. 772–776 Vol.1.
- [6] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, First 2009.
- [7] M. López-Benítez and F. Casadevall, “Improved energy detection spectrum sensing for cognitive radio,” *IET communications*, vol. 6, no. 8, pp. 785–796, 2012.
- [8] S. Atapattu, C. Tellambura, and H. Jiang, “Energy Detection Based Cooperative Spectrum Sensing in Cognitive Radio Networks,” *IEEE*

Transactions on Wireless Communications, vol. 10, no. 4, pp. 1232–1241, April 2011.

- [9] A. Mariani, A. Giorgetti, and M. Chiani, “Effects of Noise Power Estimation on Energy Detection for Cognitive Radio Applications,” *IEEE Transactions on Communications*, vol. 59, no. 12, pp. 3410–3420, December 2011.
- [10] B. Shent, L. Huang, C. Zhao, Z. Zhou, and K. Kwak, “Energy Detection Based Spectrum Sensing for Cognitive Radios in Noise of Uncertain Power,” in *2008 International Symposium on Communications and Information Technologies*, Oct 2008, pp. 628–633.
- [11] S. Enserink and D. Cochran, “A cyclostationary feature detector,” in *Proceedings of 1994 28th Asilomar Conference on Signals, Systems and Computers*, vol. 2, Oct 1994, pp. 806–810 vol.2.
- [12] K. Kim, I. A. Akbar, K. K. Bae, J. S. Um, C. M. Spooner, and J. H. Reed, “Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio,” in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 212–215.
- [13] A. Tkachenko, D. Cabric, and R. W. Brodersen, “Cyclostationary Feature Detector Experiments Using Reconfigurable BEE2,” in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 216–219.
- [14] S. Maleki, A. Pandharipande, and G. Leus, “Two-stage spectrum sensing for cognitive radios,” in *2010 IEEE International Conference on Acoustics, Speech and Signal Processing*, March 2010, pp. 2946–2949.

- [15] W. Yue and B. Zheng, “A two-stage spectrum sensing technique in cognitive radio systems based on combining energy detection and one-order cyclostationary feature detection,” in *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA09)*, 2009, pp. 327–330.
- [16] P. D. Sutton, K. E. Nolan, and L. E. Doyle, “Cyclostationary Signatures for Rendezvous in OFDM-Based Dynamic Spectrum Access Networks,” in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 220–231.
- [17] S. M. Mishra, S. ten Brink, R. Mahadevappa, and R. W. Brodersen, “Cognitive Technology for Ultra-Wideband/WiMax Coexistence,” in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, April 2007, pp. 179–186.